THE COMMITTEE ON ENERGY AND COMMERCE

INTERNAL MEMORANDUM

March 27, 2012

The Subcommittee on Commerce, Manufacturing and Trade will hold a hearing on "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?" on Thursday, March 29, 2012, at 10:00 a.m. in room 2123 of the Rayburn House Office Building. Witnesses are by invitation only.

I. Witnesses

Two Panels of witnesses will testify before the Committee.

Panel I

The Honorable Jon Leibowitz
Chairman
Federal Trade Commission (FTC)

The Honorable Lawrence E. Strickling
Assistant Secretary for Communication and Information
U.S. Department of Commerce

Panel II

Mr. Berin Szoka
President
TechFreedom

Ms. Pam Horan
President
Online Publishers Association

Mr. Jonathan Zuck
President
Association for Competitive Technology

Mr. Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

Mr. Mike Zaneis
Senior Vice President and General Counsel
Interactive Advertising Bureau

II. Background

The purpose of this hearing is to examine the White House proposal for consumer privacy, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation and the Global Digital Economy" (framework) and receive the views of stakeholders.

On February 23, 2012, the White House released its privacy framework based largely on the efforts of the National Telecommunications and Information Administration (NTIA) and the FTC over the past several years. The NTIA originally released a "Green Paper" in December 2010 based on its Internet Policy Task Force inquiry regarding information privacy and innovation in the Internet. In that report, the Task Force made recommendations for building a general privacy framework based on an expanded set of Fair Information Practice Principles, the publication of privacy impact assessments by industry, the use of voluntary codes of conduct to address emerging technologies, and the establishment of a Privacy Policy Office within the Department of Commerce.

Similarly, the FTC has been active on privacy and focused much attention on Internet privacy in more recent years. The Commission issued a staff report entitled "Self-Regulatory Principles for Online Behavioral Advertising" in February 2009,[1] followed by a preliminary staff report in December 2010 titled "Protecting Consumer Privacy in an Era of Rapid Change".[2] The Commission has collected extensive public comments on that report and plans to issue a final report this month.

III. Summary of the Framework

The framework's stated purpose is to ensure consumer trust in networked technologies by addressing two areas the Administration finds lacking: a clear statement of privacy principles applicable to the commercial world and a "sustained commitment of all stakeholders to address consumer privacy issues as they arise from advances in technological and business models".[3]

The framework hinges on these elements: (1) a consumer privacy "bill of rights"; (2) a multi-stakeholder process for developing enforceable codes of conduct; (3) FTC enforcement; and (4) increased international interoperability.

---

[1] Available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.
[2] Available at http://ftc.gov/os/2010/12/101201privacyreport.pdf.
[3] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation and the Global Digital Economy, "Forward" available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

A. Consumer Privacy Bill of Rights

The privacy bill of rights provides seven principles regarding personal data:

- **Individual Control:** Customers have the right to exercise control over what personal data companies collect about them and how they use it.
    - Companies should provide consumers with control, including choice at the time of collection, appropriate to the scale, scope and sensitivity of the data (i.e., for more sensitive data, more granular control may be appropriate). The principle also includes the right to withdraw consent in a similar manner as originally provided.
- **Transparency**: Consumers have a right to easily understandable and accessible information about privacy and security practices.
    - Companies should give the consumer timely and clear descriptions of what data they will collect, why they collect it, how they will use it, when they will delete it and whether and for what purposes they will share it with third parties.
- **Respect for Context**: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
    - Companies should limit their use and disclosure of data to purposes consistent with the relationship and context in which the data was collected. If companies later wish to use or disclose personal data for purposes inconsistent with the original context in which it was disclosed, they must provide a heightened degree of notice and choice. Companies should meet the principle in ways appropriate for the age and sophistication of the consumers. Companies may infer consent for purposes such as order fulfillment and most first-party marketing as well as other purposes including analytics and fraud prevention.
- **Security**: Consumers have a right to secure and responsible handling of personal data.
    - Companies should maintain reasonable safeguards, commensurate with the type and sensitivity of the data they hold, to control against risk of loss, theft, or improper disclosure.
- **Access and Accuracy**: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.

- Companies should reasonably ensure they maintain accurate data and provide consumers reasonable access to personal data they collect as well as the ability to correct inaccurate information or request its deletion.

- **Focused Collection**: Consumers have a right to reasonable limits on the personal data that companies collect and retain.

  - Companies should consider the kinds of information they need to accomplish specific purposes. Companies may develop new uses for data they collect, provided they take appropriate measures of notice and individual choice.

- **Accountability**: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

  - Companies should be accountable to enforcement authorities and consumers for adherence to the principles**.** Companies should conduct full audits, where appropriate, and ensure third parties with whom they share personal data are under enforceable contracts. Accountability should include internal practices that maintain compliance or detect and remedy any lapses that occur.

B. Multi-Stakeholder Process to Develop Enforceable Codes of Conduct

The framework posits an open, transparent process, facilitated by the NTIA, to implement the principles through more specific practices. The Administration believes a multi-stakeholder process, if appropriately structured, can provide the necessary flexibility, speed and decentralization to address Internet policy. The Administration encourages stakeholder representatives from companies, industry groups, privacy advocates, consumer groups, State Attorneys General, and Federal civil and criminal law enforcement agencies to participate.

Regardless of whether legislation is passed, the Administration is moving forward to convene the multi-stakeholder process. In fact, the NTIA issued a formal request for comment on February 29, 2012, regarding both substantive consumer data privacy issues that warrant codes of conduct as well as the procedures to foster the development of the codes.[4] The deadline for comments was originally March 26, but has since been extended until April 2, 2012.

Based on the success of existing multi-stakeholder processes, including private-sector standard setting organizations that have developed Internet technical standards, the Administration believes there are definite benefits for stakeholders to participate. Of relevance to

[4] Available at http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf

companies is favorable consideration by the FTC in any enforcement action based on conduct covered by the code. However, the choice to adopt the codes will be voluntary.[5]

The NTIA will play a significant role as the convener of the process. It is envisioned that the agency will help identify issues and industry sectors that are candidates for codes of conduct and facilitate deliberations that conclude with agreement of all stakeholders on a code of conduct companies may adopt.

C. Enforcement

The FTC and State attorneys general have brought enforcement actions against companies that have failed to adhere to voluntary codes of conduct developed through multi-stakeholder process, including privacy policies, and for failure to adequately protect personal data. Similarly, the FTC and State attorneys general could enforce the voluntary codes of conduct in the same manner.

D. International Interoperability

The importance of cross border data flows can be challenged by different national privacy laws. The framework intends to facilitate transnational mutual recognition of privacy regimes to increase interoperability of privacy laws. The Administration believes the codes of conduct implementing the Privacy Bill of Rights can build on the Safe Harbor Frameworks the U.S. developed with the EU to allow U.S. companies to comply with the EU Data Protection Directive, and will further interoperability because they will address sectors not regulated by the FTC, and therefore not covered by the Safe Harbor Frameworks. The Administration hopes to include international stakeholders in the multi-stakeholder process to further garner international consensus.

E. Additional Provisions

The Framework also calls on Congress to:

a. Adopt the Privacy Bill of Rights through codifying legislation.
b. Grant the FTC authority to enforce each element of the statutory Consumer Privacy Bill of Rights through baseline privacy legislation.
c. Provide legal certainty through an enforcement safe harbor by Congress granting the FTC new authority. First, the FTC would have authority to review codes of conduct against the Consumer Privacy Bill of Rights, and after public comment, either accept or reject each one. Second, the FTC would have authority to grant a safe harbor to companies who follow a code the FTC has approved.

[5] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation and the Global Digital Economy, p.24, p.30 available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

d. Create a national uniform set of rules that preempts State laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights as enacted and applied and provide forbearance from State enforcement of State laws against companies that adopt and comply with FTC approved codes of conduct, but allow States to enforce the Privacy Bill of Rights.
e. Preserve existing effective sector-specific privacy laws (e.g., HIPAA, COPPA, FCRA) but seek to simplify existing or duplicative requirements, including making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers.
f. Create a national data breach notification standard to replace the variations in the existing 47 State breach notification laws.

Please contact Brian McCullough, Gib Mullan, or Shannon Weinberg at (202) 225-2927 with any questions.